REMARKS

Claims 7-13, 17-19 and 21-31 are pending.

Claim 21-26 are rejected under 35 U.S.C. § 112 as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Claims 7-12, 21-22, 24-25, and 30 are rejected under 35 U.S.C. § 103(a) as being unpatentable over Gupta et al. (U.S. Patent No. 6,389,532, hereinafter referred to as Gupta) in view of Hakim et al. (U.S. Patent Pub. No. 2002/0167943, hereinafter referred to as Hakim).

Claims 13, 17-19, 23, 26-29, and 31 are rejected under 35 U.S.C. §103(a) as being unpatentable over Gupta in view of Hakim, and further in view of Gibbs et al. (U.S. Patent No. 6,085,321, hereinafter referred to as Gibbs).

Claims 17, 21, 23, 27, and 31are amended.

Claims 7-13, 17-19 and 21-31 remain in the case for reconsideration.

The applicant adds no new matter and request reconsideration in light of the above amendments and the following remarks.

Claim Rejections – 35 U.S.C. § 112

Claims 21-26 are rejected for insufficient antecedent basis. The applicant amends claim 21 to include proper antecedent basis. Therefore, claim 21 and its dependent claims 22-26 are in condition for allowance in this regard.

Claim Rejections – 35 U.S.C. § 103

Claims 7-12, 21-22, 24-25, and 30 are rejected as being obvious over Gupta in view of Hakim. The applicant disagrees for the reasons that follow.

Claim 7 recites *transmitting the content file when data comprising the content file does not include the restricted data format.* Claim 30 includes similar limitations as in claim 1.

The Examiner acknowledges that Gupta does not teach the above limitation. Office Action, Page 3. The Examiner, however, alleges that Hakim discloses such feature, citing FIG. 6, Ref. 612.

Hakim's 612 of FIG. 6 does not teach transmitting the content file when data comprising the content file does not include the restricted data format as taught in claim 1. Hakim's 612 in FIG. 6 teaches "Destination receives call and caller is connected." In other words, Ref. 612 of FIG. 6 merely discloses that the content file is transmitted to the destination regardless of whether the content file includes the restricted data format or not.

The Examiner further alleges that it would be obvious to modify Gupta to "provide security to prevent sensitive information, such as, to be transmitted." Office Action, Page 4. But there is no such suggestion or motivation to combine the reference teachings.

Gupta teaches a method for using digital signatures to filter packets in a network in order to prevent wasting of network resources associated with unauthorized senders in a multicast context. See Abstract, and Col. 1, lines 56-62. In Gupta, data are encrypted, and only the authorized group members can decrypt the data using a group key. Col. 1, lines 34-36. As such, Gupta does not require or benefit from Hakim's firewall to prevent sensitive information to be transmitted, because Gupta's data are already encrypted and secured. Therefore, no such motivation exists to combine these teachings and the combination of Gupta and Hakim is invalid. Accordingly, Claims 7 and 30 and their respective dependent claims are allowable.

Claim 21 recites *blocking transmission of the content file when the content file does not include the digital signature* *to prevent unauthorized downloading of copyrighted material*...

The Examiner alleges that Gupta teaches the above limitation, citing Col. 4, lines 12-13. Gupta, however, does not teach blocking transmission of the content file when the content file does not include the digital signature to prevent unauthorized downloading of copyrighted material. Gupta teaches blocking transmission of a packet when the packet does not bear a valid digital signature or the packet does not contain a signature when one is required, to avoid wasting router bandwidth and resources on processing packets associated with unauthorized senders. See FIG. 7, steps 706, 710, 718, 722, and Col. 1, lines 56-62. That is, Gupta discards packets from unauthorized senders who may cause a network bottleneck by sending numerous unauthorized messages to an end host of a system in the network. See Col. 1, lines 47-55. Gupta thus teaches preventing unauthorized sending from unauthorized senders regardless of whether the material is copyrighted or not. Gupta does not teach preventing unauthorized downloading of protected/copyrighted material.

Claim 21 further recites *blocking transmission of the content file when the content file does not include the digital signature to prevent unauthorized downloading of copyrighted material, wherein the blocking is effected prior to a transmission of the content file to a receiver.*

The Examiner acknowledges that Gupta does not teach the above limitation. Office Action, Page 3. The Examiner, however, alleges that Hakim teaches this limitation, citing Paragraph [0099]. But as discussed above, Gupta does not require or benefit from Hakim's firewall to prevent sensitive information to be transmitted, since Gupta's data are already encrypted and secured. Therefore, there is no suggestion or motivation to combine the reference teachings and there is no reason to try to make the proposed combination of Gupta and Hakim. Claims 21 and its dependent claims are allowable.

Claim Rejections – 35 U.S.C. § 103

Claims 13, 17-19, 23, 26-29, and 31 are rejected as being obvious over Gupta in view of Hakim, and further in view of Gibbs. The applicant disagrees for the reasons that follow.

Claim 17 recites *using at least one router configured to log digital signatures related to the digital content file to maintain a record for the digital content file and related digital signatures*.... Claims 23, 27 and 31 include similar limitations.

The Examiner acknowledges that the combination of Gupta as modified by Hakim does not teach the above limitation. Office Action, Page 9. The Examiner, however, alleges that Gibbs teaches the limitation, citing FIG. 4, Ref. 432, and Col. 6, lines 17-26. Gibbs does not teach logging digital signatures related to the digital content file to maintain a record for the digital content file and related digital signatures.

As shown in FIG. 2, Gibb teaches an authentication log file 200 (also referred to as authentication log file 432 in FIG. 4), which comprises a plurality of exemplary records (204, 208, 212, 216 and 220). Each record of the authentication log file 200 contains three fields: system key number field 230, which points to a corresponding record of the authentication log file 200; system key field 234 that stores the system key 108, which is a 256 bit value that changes periodically and is randomly generated by the authenticated message server 100; and status field 240, which is a bit vector for storing status information about each of the unique

digital signatures successfully authenticated by the authenticated message server 100. See Col. 4, lines 10-22, and Col. 3, lines 50-52. None of the fields in Gibbs' log file maintains a record for the digital content file and related digital signatures as recited in claims 17, 23, 27, and 31.

Gibbs adds nothing to overcome the deficiencies in Gupta and Hakim. Consequently, Gupta and Hakim in view of Gibbs does not render obvious all of the limitations as set forth in claims 17, 23, 27, and 31. Accordingly, claims 17, 23, 27, and 31 and their respective dependent claims are allowable.

Claim 13 recites *the examining is performed by a plurality of cache engines within the distributed computer network.* Claim 26 includes similar limitations.

The Examiner acknowledges that the combination of Gupta as modified by Hakim does not teach the above limitation. Office Action, Page 10. The Examiner, however, alleges that Gibbs teaches examining performed by a plurality of cache engines with the distributed network as in claims 13 and 26, citing FIG. 4, Ref. 420, and Col. 7, lines 13-28. But Gibbs's proxy server 420 does not teach examining data comprising the content file to determine whether the content file includes a restricted data format as recited in claim 13, nor does Gibbs teach examining the content file to determine whether the content file includes the digital signature as in claim 26. Instead, Gibbs' proxy server 420 is "a high-speed cache for one or more internet servers (e.g., WWW server 424) connected to the LAN 436. Functionally, the proxy server 420 strips off the prefix of any URLs received and compares the remaining URL to datafiles stored in its cache. If there is a match, then, rather than requesting the datafile from the WWW server 424 (which is generally more expensive in terms of processing time and I/O), the cached copy I/O on the proxy server 420 is spooled out to the requester, thereby saving a disk I/O and time." Col. 7, lines 13-25.

Gibbs adds nothing to overcome the deficiencies in Gupta and Hakim. Consequently, Gupta and Hakim in view of Gibbs does not render obvious the limitations as set forth in claims 13 and 26. Accordingly, claims 13 and 26 are allowable.

In view of the foregoing amendments and remarks, applicant believes the application should be in condition for allowance. If any questions remain, the Examiner is requested to call the undersigned.

Respectfully submitted,

20575
Customer No.

MARGER JOHNSON & McCOLLOM, P.C.

By _____
Alexander C. Johnson, Jr.
Registration No. 29,396

210 S.W. Morrison Street, Suite 400
Portland, Oregon 97204
Telephone: (503) 222-3613